KOPELOWITZ OSTROW P.A.
Kristen Lake Cardoso (CA Bar No. 338762)
cardoso@kolawyers.com
Jeff Ostrow (*pro hac vice* forthcoming)
ostrow@kolawyers.com
One West Las Olas, Suite 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100

Counsel for Plaintiff and the Proposed Class

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

RANDALL WRIGHT, *individually and on behalf of all others similarly situated*,

Plaintiff,

v.

SMART ERP SOLUTIONS, INC.,

Defendant.

Case No.

CLASS ACTION

CLASS ACTION COMPLAINT FOR DAMAGES

1. **Negligence/Negligence *Per Se***
2. **Unjust Enrichment**
3. **Breach of Third-Party Beneficiary Contract**

DEMAND FOR JURY TRIAL

Plaintiff Randall Wright ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Defendant Smart ERP Solutions, Inc. ("Defendant"), alleging as follows based upon personal knowledge, information and belief, and investigation of counsel.

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and Class Members' sensitive personally identifying information ("PII"),[1] which, as a result, is now in criminal cyberthieves' possession.

2. Between July 3 and July 13, 2024, hackers targeted and accessed Defendant's network systems and stole Plaintiff's and Class Members' sensitive, confidential PII stored therein, including their full names in combination with Social Security numbers, and other sensitive data, causing widespread injuries to Plaintiff and Class Members (the "Data Breach").

3. Defendant provides enterprise resource planning software and services related to human resources, sales, logistics, data management, and other functions to its corporate clients across the United States.[2]

4. Plaintiff and Class Members are current and former customers and/or employees of Defendant's clients who were and are required to entrust Defendant with their sensitive, non-public PII. Defendant could not perform its operations or provide its services without collecting Plaintiff's and Class Members' PII and retains it for many years, at least, even after Plaintiff's and Class Members' relationships with Defendant's clients ended.

[1] The Federal Trade Commission ("FTC") defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth. . . .." 17 C.F.R. § 248.201(b)(8).

[2] *See* About Us, https://www.smarterp.com/company/about-us.

5. Businesses like Defendant that handle PII owe the individuals to whom that data relates a duty to adopt reasonable measures to protect such information from disclosure to unauthorized third parties, and to keep it safe and confidential. This duty arises under contract, statutory and common law, industry standards, representations made to Plaintiff and Class Members, and because it is foreseeable that the exposure of PII to unauthorized persons—and especially hackers with nefarious intentions—will harm the affected individuals, including but not limited to by the invasion of their private health matters.

6. Defendant breached these duties owed to Plaintiff and Class Members by failing to safeguard their PII it collected and maintained, including by failing to implement industry standards for data security to protect against, detect, and stop cyberattacks, which failures allowed criminal hackers to access and steal thousands of consumers' PII from Defendant's care.

7. According to Defendant's notice of the Data Breach provided to Data Breach victims ("Notice Letter"), between July 3, 2024 and July 13, 2024, unknown, unauthorized actors hacked into Defendant's network systems and accessed and/or acquired files containing Plaintiff's and Class Members' PII.

8. Although the Data Breach took place in July 2024, Defendant failed to notify affected individuals that their PII was compromised until approximately March 11, 2024—***over 8 months*** later—diminishing Plaintiff's and Class Members' ability to timely and thoroughly mitigate and address the increased, imminent risk of identity theft and other harms the Data Breach caused.

9. Defendant failed to adequately protect Plaintiff's and Class Members' PII, and failed to even encrypt or redact this highly sensitive data. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect consumers' sensitive data.

10. Defendant maintained the PII in a reckless manner. In particular, PII was maintained on and/or accessible from Defendant's employee email accounts in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus, Defendant knew that failing to take reasonable steps to secure the PII left it in a dangerous condition.

11. Hackers targeted and obtained Plaintiff's and Class Members' PII from Defendant's accounts because of the data's value in exploiting and stealing identities. As a direct and proximate result of Defendants' inadequate data security and breaches of its duties to handle PII with reasonable care, Plaintiff's and Class Members' PII has been accessed by hackers and exposed to an untold number of unauthorized individuals. The present and continuing risk to Plaintiff and Class Members will remain for their respective lifetimes.

12. The harm resulting from a cyberattack like this Data Breach manifests in numerous ways including identity theft and financial fraud, and the exposure of an individual's PII due to a data breach ensures that the individual will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of his or her life. Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take several additional prophylactic measures.

13. As a result of the Data Breach, Plaintiff and Class Members suffered and will continue to suffer concrete injuries in fact, including but not limited to (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) actual identity theft and fraud; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred

due to actual identity theft; (f) deprivation of value of their PII; (g) loss of privacy; (h) emotional distress including anxiety and stress in with dealing with the Data Breach; and (i) the continued risk to their sensitive PII, which remains in Defendant's possession and subject to further breaches, so long as Defendant fails to undertake adequate measures to protect the customer data it collects and maintains.

14. To recover from Defendant for these harms, Plaintiff, on his own behalf and on behalf of the Class as defined herein, brings claims for negligence/negligence per se, unjust enrichment, and breach of third-party beneficiary contract to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' PII.

15. Plaintiff and Class Members seek damages and equitable relief requiring Defendant to (a) disclose the full nature of the Data Breach and types of PII exposed; (b) implement data security practices to reasonably guard against future breaches; and (c) provide, at Defendant's expense, all Data Breach victims with lifetime identity theft protection services.

PARTIES

Plaintiff Randall Wright

16. Plaintiff is an adult individual who at all relevant times has been a citizen and resident of Coweta County, Georgia.

17. Plaintiff is a former customer of Defendant and received financial services from Defendant prior to the Data Breach. Plaintiff provided his PII to Defendant as a condition of and in exchange for obtaining services from Defendant.

18. Plaintiff greatly values his privacy and is very careful about sharing his sensitive PII. Plaintiff diligently protects his PII and stores any documents containing PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff

would not have provided his PII to Defendant had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

19. At the time of the Data Breach, Defendant retained Plaintiff's PII in its employee email accounts and network systems with inadequate data security, causing Plaintiff's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

20. On or about March 11, 2025, Plaintiff received Defendant's Notice Letter informing that his PII was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers acquired files containing Plaintiff's sensitive PII, including his name in combination with his Social Security number.

21. Plaintiff further believes his PII, and that of Class Members, was and will be sold and disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

22. Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff now monitors his financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

23. Plaintiff further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff is at a present risk and will continue to be at risk of identity theft and fraud for years.

24. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff's and Class Members' PII was targeted, accessed, and

misused, including through present and/or imminent publication and dissemination on the dark web.

25. The Data Breach also caused Plaintiff to suffer fear, anxiety, and stress about his PII now being in the hands of cybercriminals, compounded by the fact that Defendant still has not fully informed him of key details about the Data Breach's occurrence or the information stolen.

Defendant Smart ERP Solutions, Inc.

26. Defendant is a California corporation with its headquarters and principal place of business at 3875 Hopyard Road, Suite 180, Pleasanton, CA 94588.

JURISDICTION AND VENUE

27. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because the amount in controversy exceeds $5 million, exclusive of interest and costs, the number of Class Members is over 100, and at least one Class Member, namely, Plaintiff, is a citizen of a state that is diverse from Defendant's citizenship. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

28. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is located in this District, and a substantial part of the events giving rise to this action and Plaintiff's claims occurred in this District.

FACTUAL BACKGROUND

A. Defendant Owed Duties to Adopt Reasonable Data Security Measures for PII it Collected and Maintained.

29. Defendant provides enterprise resource planning software to its corporate clients across the United States.[3]

[3] *See* About Us, https://www.smarterp.com/company/about-us.

30. Plaintiff and Class Members are current and former customers and/or employees of Defendant's clients, who were required to provide Defendant, directly or indirectly, with their highly sensitive PII.

31. The information Defendant held in its computer networks at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

32. At all relevant times, Defendant knew it was storing and using its networks to store and transmit valuable, sensitive PII belonging to Plaintiff and Class Members, and that as a result, its systems would be attractive targets for cybercriminals.

33. Defendant also knew that any breach of its information technology network and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the individuals whose PII was compromised, as well as intrusion into those individuals' highly private financial information.

34. Defendant owed duties to the individuals to whom the PII Defendant collected and stored maintained, including Plaintiff and Class Members, to keep the PII Defendant collected from them safe and confidential, to maintain the privacy of that information, and to delete any sensitive information after Defendant was no longer required to maintain it.

35. Plaintiff and Class Members provided their PII to Defendant, directly or indirectly, with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and protected against unauthorized access.

36. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII. To that end, Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

37. Defendant derived economic benefits from collecting Plaintiff's and Class Members' PII, including payment for providing data management services

specifically. Without the required submission of PII, Defendant could not provide its services or generate revenue.

38. By obtaining, using, and benefiting from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting that PII from unauthorized access and disclosure.

39. Defendant had and has a duty to adopt reasonable measures to keep Plaintiff's and Class Members' PII confidential and protected from involuntary disclosure to third parties, and to audit, monitor, and verify the integrity of its IT networks, and train employees with access to use adequate cybersecurity measures.

40. Defendant had and has obligations created by the FTC Act, 15 U.S.C. § 45, common law, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and protected from unauthorized disclosure. Defendant failed to do so.

B. Defendant Failed to Adequately Safeguard Plaintiff's and Class Member's PII, Causing the Data Breach.

41. On or about March 11, 2025, Defendant began sending Plaintiff and other Data Breach victims Notice Letters informing them of the Data Breach.[4]

42. The Notice Letters generally inform as follows, in part:

> *What Happened?*
> On July 13, 2024, Smart ERP experienced a network security incident that impacted some operations.
>
> *What We Are Doing.*
> . . . After an extensive investigation and manual document review, on February 11, 2025, we discovered that between July 3, 2024 and July 13, 2024, a limited amount of information on our network may have been accessed and/or acquired by an unauthorized individual.
>
> *What Information Was Involved?*
> The impacted information includes the following: full name and Social Security number.

[4] *See* Notice Ltr., Ex. A.

43. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII is protected.

44. Thus, Defendant's purported 'disclosure' amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

45. To make matters worse, although the Data Breach occurred up to July 13, 2024, Defendant waited until March 11, 2025, before it began notifying affected individuals about their PII being compromised, diminishing Plaintiff's and Class Members' ability to timely and thoroughly mitigate and address harms resulting from the unauthorized disclosure.

46. Plaintiff's and Class Members' PII was targeted, accessed, and stolen by cybercriminals in the Data Breach. Criminal hackers accessed and acquired confidential files containing Plaintiff's and Class Members' PII from Defendant's email accounts, where they were kept without adequate safeguards and in unencrypted form.

47. Defendant could have prevented this Data Breach by properly training personnel, securing account access through measures like phishing-resistant (i.e., non-SMS text based) multi-factor authentication ("MFA") for as many services as possible, training users to recognize and report phishing attempts, implementing recurring forced password resets, and/or securing and encrypting files and file servers containing Plaintiff's and Class Members' PII, but failed to do so.

48. As the Data Breach evidences, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive PII it collected and maintained from Plaintiff and Class Members, such as phishing-resistant MFA, standard monitoring and altering techniques, encryption, or deletion of information when it is no longer needed. These failures by Defendant allowed and caused cybercriminals to target Defendant's network, access it without permission for days, and exfiltrate files containing Plaintiff and Class Member's PII.

49. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing Plaintiff's and Class Members' PII, using controls like limitations on personnel with access to sensitive data and requiring phishing-resistant MFA for access, training its employees on standard cybersecurity practices, and implementing reasonable logging and alerting methods to detect unauthorized access.

50. For example, if Defendant had implemented industry standard logging, monitoring, and alerting systems—basic technical safeguards that any PHI and/or PII-collecting company is expected to employ—then cybercriminals would not have been able to perpetrate malicious activity in Defendant's network systems for the period it took to carry out the Data Breach, including the reconnaissance necessary to identify where Defendant stored PII, installation of malware or other methods of establishing persistence and creating a path to exfiltrate data, staging data in preparation for exfiltration, and then exfiltrating that data outside of Defendant's system without being caught.

51. Defendant would have recognized the malicious activities detailed in the preceding paragraph if it bothered to implement basic monitoring and detection systems, which then would have stopped the Data Breach or greatly reduced its impact.

52. Further, upon information and belief, had Defendant required phishing-resistant MFA, and/or trained its employees on reasonable and basic cybersecurity topics like common phishing techniques or indicators of a potentially malicious event, cybercriminals would not have been able to gain initial access to Defendant's network or Plaintiff's and Class Members' PII through.

53. Defendant's tortious conduct and breach of contractual obligations, as detailed herein, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed Plaintiff's and Class Members' PII, meaning Defendant had no effective means in place to ensure that cyberattacks were detected and prevented.

C. Defendant Knew of the Risk of a Cyberattack because Businesses in Possession of PII are Particularly Suspectable.

54. Defendant's negligence in failing to safeguard Plaintiff's and Class Members' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing such data.

55. PII of the kind accessed in the Data Breach is of great value to hackers and cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the dark web.

56. PII can also be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and financial records. This may be accomplished alone, or in combination with other personal information that is connected, or linked to an individual, such as his or her birthdate, birthplace, and mother's maiden name.

57. Data thieves regularly target entities in the technology and data management industry like Defendant due to the highly sensitive information that such entities maintain. Defendant knew and understood that unprotected PII is

valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

58. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole.[5]

59. Cyber-attacks against businesses such as Defendant are targeted and frequent. According to Contrast Security's 2023 report *Cyber Bank Heists: Threats to the financial sector*, "Over the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[6] In fact, "40% [of financial institutions] have been victimized by a ransomware attack."[7]

60. In light of past high profile data breaches at industry-leading companies, including, for example, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or, if acting as a reasonable financial institution, should have known that the PII it collected and maintained would be vulnerable to and targeted by cybercriminals.

61. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data

[5] *Id.*

[6] Contrast Security, "Cyber Bank Heists: Threats to the financial sector," pg. 5, avail. at https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%2020 23.pdf?hsLang=en (last acc. February 9, 2024).

[7] *Id.*, at 15.

events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[8]

62. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant itself. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[9]

63. As a businesses in possession of its clients' customers' and/or employees' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. Such consequences include the significant costs imposed on Plaintiff and Class Members due to a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

64. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being wrongfully disclosed to cybercriminals.

65. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class Members' PII compromised therein would be targeted by hackers and cybercriminals for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' PII can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiff's and Class Members' names.

[8] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data- breach-report-sets-new-record-for-number-of-compromises/ (last accesses Feb. 9, 2024).

[9] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last accessed Feb. 9, 2024).

66. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its network server(s), amounting to tens of thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of that unencrypted data.

67. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing PII and the critical importance of providing adequate security for that information.

68. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, credit and bank fraud, and the like.

D. Defendant was Required, but Failed to Comply with FTC Rules and Guidance.

69. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

70. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses like Defendant. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[10]

[10] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016),https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed May 8, 2024).

71. The FTC's guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[11]

72. The FTC further recommends that companies not maintain confidential personal information, like PII, longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

73. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures business like Defendant must undertake to meet their data security obligations.

74. Such FTC enforcement actions include actions against businesses that fail to adequately protect consumer PII like Defendant. *See, e.g., In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

75. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the

[11] *Id.*

unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect sensitive personal information, like PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

76. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[12]

77. Defendant failed to properly implement basic data security practices, in violation of its duties under the FTC Act.

78. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

E. Defendant Failed to Comply with Industry Standards.

79. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

80. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log

[12] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[13]

81. In addition, the NIST recommends certain practices to safeguard systems[14]:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

82. Further still, the Cybersecurity & Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing]

[13] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. Feb. 9, 2024).

[14] Federal Trade Commission, "Understanding The NIST Cybersecurity Framework," https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist- framework (last acc. Feb. 9, 2024).

that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[15]

83. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiff's and Class Members' PII, resulting in the Data Breach.

F. Defendant Owed Plaintiff and Class Members a Common Law Duty to Safeguard their PII.

84. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized

[15] Cybersecurity & Infrastructure Security Agency, "Shields Up: Guidance for Organizations," available at https://www.cisa.gov/shields-guidance-organizations (last acc. Feb. 9, 2024).

persons. Defendant's duty owed to Plaintiff and Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure its computer systems, networks, and protocols adequately protected Plaintiff's and Class Members' PII.

85. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

86. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of PII in a timely manner and act upon data security warnings and alerts in a timely fashion.

87. Defendant owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

88. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

89. Defendant failed to take the necessary precautions required to safeguard and protect Plaintiff's and Class Members' PII from unauthorized disclosure. Defendant's actions and omissions represent a flagrant disregard of Plaintiff's and Class Members' rights.

G. Plaintiff and Class Members Suffered Common Injuries and Damages due to Defendant's conduct.

90. Defendant's failure to implement or maintain adequate data security measures for Plaintiff's and Class Members' PII directly and proximately injured Plaintiff and Class Members by the resulting disclosure of their PII in the Data Breach.

91. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen fraudulent use of that information and damage to victims may continue for years.

92. Plaintiff and Class Members are also at a continued risk because their Private remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its customers' PII.

93. As a result of Defendant's ineffective and inadequate data security practices, the resulting Data Breach, and the foreseeable consequences of their PII ending up in criminals' possession, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and they have all sustained actual injuries and damages, including, without limitation, (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their PII; (g) loss of the benefit of their bargain with Defendant; (h) emotional distress including anxiety and stress in dealing with the Data Breach's aftermath; and (i) the continued risk to their sensitive PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII it collects and maintains.

The Risk of Identity Theft to Plaintiff and Class Members is Present and Ongoing

94. Plaintiff and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

95. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[16] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[17]

96. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal individuals' personal data to monetize the information. Criminals monetize the data by selling the stolen information on the internet black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

97. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[18] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[19] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

98. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical

[16] 17 C.F.R. § 248.201 (2013).
[17] *Id.*
[18] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[19] *Id.*

information like the PII at issue here.[20] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[21] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[22]

99. The unencrypted PII of Plaintiff and Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted and detailed PII may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Plaintiff's and Class Members' PII.

100. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

101. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing

[20] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[21] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[22] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

102. Identity thieves can also use an individual's personal data and PII to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's information, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name.[23]

103. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[24]

104. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

---

[23] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[24] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/ medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited Feb. 26, 2024).

105. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

106. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

107. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

108. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that their stolen PII is being misused, and that such misuse is traceable to the Data Breach.

109. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect

losses are included in the calculation of out-of-pocket loss.[25]

110. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[26]

111. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[27] Yet, Defendant failed to rapidly report to Plaintiff and the Class that their PII was stolen.

112. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

113. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

114. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

[25] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Jan. 23, 2024).
[26] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.
[27] *Id.*

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

115. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

116. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record

117. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate that harm.

118. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

119. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies

to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[28]

120. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct that caused the Data Breach.

Diminished Value of PII

121. Personal data like PII is a valuable property right.[29] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

122. An active and robust legitimate marketplace for personal information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[30] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[31, 32] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[33]

[28] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Feb. 26, 2024).

[29] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[30] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[31] https://datacoup.com/.

[32] https://digi.me/what-is-digime/.

[33] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

123. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and black markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for the threat actors.

124. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

125. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered due to the Data Breach.

126. Given the type of targeted attack in this case and sophisticated criminal activity, the type of information involved, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or insurance; or filing false unemployment claims.

127. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

128. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel their cards and

request a replacement.[34] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

129. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

130. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

CLASS ACTION ALLEGATIONS

131. Plaintiff brings this nationwide class action on behalf of himself and all others similarly situated pursuant to Federal Rule of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

132. Plaintiff proposes the following nationwide class definition, subject to amendment based on information obtained through discovery:

> **All persons in the United States whose Private Information was compromised in the Data Breach, including all persons who received a Notice Letter ("Class").**

133. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

[34] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

134. Numerosity. The Class members are so numerous that joinder of all of them is impracticable. While the precise number of Class members at issue has not been determined, Plaintiff believes the Data Breach affects at least thousands of individuals.

135. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether unauthorized hackers obtained Class Members' PII in the Data Breach;

h. Whether Defendant knew or should have known its data security systems and monitoring processes were deficient;

i. Whether Defendant's conduct was negligent;

j. Whether Defendant's conduct was in violation of the FTC Act such that Defendant was negligent *per se*;

k. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

l. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

136. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

137. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff's Counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

138. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

139. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer

management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

140. Class certification is also appropriate because Defendant has acted or refused to act on grounds that apply generally to the Class as a whole, so that class certification, final injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

141. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. At least some Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

COUNT I

NEGLIGENCE/NEGLIGENCE *PER SE*

(On Behalf of Plaintiff and the Class)

142. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 141 above as if fully set forth herein.

143. Defendant required Plaintiff and Class Members to submit, directly or indirectly, sensitive, confidential PII to Defendant.

144. Plaintiff and Class Members provided their PII to Defendant, including their full names, Social Security numbers, and other sensitive data.

145. Defendant had full knowledge of the sensitivity of the PII to which it was entrusted, and the types of harm that Plaintiff and Class Members could and would suffer if the PII was wrongfully disclosed to unauthorized persons.

146. Defendant owed a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting the PII it collected from them.

147. Plaintiff and Class Members were the foreseeable victims of any inadequate data safety and security practices by Defendant.

148. Plaintiff and Class Members had no ability to protect their PII in Defendant's possession.

149. By collecting, transmitting, and storing Plaintiff's and Class Members' PII Defendant owed Plaintiff and Class Members a duty of care to use reasonable means to secure and safeguard their PII, to prevent the information's unauthorized disclosure, and to safeguard it from theft or exfiltration to cybercriminals. Defendant's duty included the responsibility to implement processes by which it could detect and identify malicious activity or unauthorized access on its networks or servers.

150. Defendant owed a duty of care to Plaintiff and the Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that controls for its networks, servers, and systems, and the personnel responsible for them, adequately protected Plaintiff's and Class Members' PII.

151. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential PII.

152. Pursuant to the FTC Act, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

153. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices and procedures to safeguard Plaintiff's and Class Members'

PII, and by failing to ensure the PII in its systems was encrypted and timely deleted when no longer needed.

154. Plaintiff's and Class Members' injuries resulting from the Data Breach were directly and indirectly caused by Defendant's violations of the FTC Act.

155. Plaintiff and Class Members are within the class of persons the FTC Act is intended to protect.

156. The type of harm that resulted from the Data Breach was the type of harm the FTC Act is intended to guard against.

157. Defendant's failure to comply with the FTC Act constitutes negligence *per se*.

158. Defendant's duty to use reasonable care in protecting Plaintiff's and Class Members' confidential PII in its possession arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to reasonably protect such PII.

159. Defendant breached its duties of care, and was grossly negligent, by acts of omission or commission, including by failing to use reasonable measures or even minimally reasonable measures to protect the Plaintiff's and Class Members' PII from unauthorized disclosure in this Data Breach.

160. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

m. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' PII;

n. Maintaining and/or transmitting Plaintiff's and Class Members' PII in unencrypted and identifiable form;

o. Failing to implement data security measures, like adequate, phishing-resistant MFA for as many systems as possible, to safeguard against

known techniques for initial unauthorized access to network servers and systems;

p. Failing to adequately train employees on proper cybersecurity protocols;

q. Failing to adequately monitor the security of its networks and systems;

r. Failure to periodically ensure its network system had plans in place to maintain reasonable data security safeguards;

s. Allowing unauthorized access to Plaintiff's and Class Members' PII; and

t. Failing to adequately notify Plaintiff and Class Members about the Data Breach so they could take appropriate steps to mitigate damages.

161. But for Defendant's wrongful and negligent breaches of its duties owed to Plaintiff and Class Members, their PII would not have been compromised because the malicious activity would have been prevented, or at least, identified and stopped before criminal hackers had a chance to inventory Defendant's digital assets, stage them, and then exfiltrate them.

162. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII would injure Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in Defendant's industry.

163. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII would cause them one or more types of injuries.

164. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injuries, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their PII; (c) actual identity theft, or the imminent and substantial risk of identity theft or fraud; (d) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual

consequences of the Data Breach, including but not limited to lost time; (e) loss of benefit of the bargain; (f) anxiety and emotional harm due to their PII's disclosure to cybercriminals; and (g) the continued and certainly increased risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it.

165. Plaintiff and Class Members are entitled to damages, including compensatory, consequential, punitive, and nominal damages, as proven at trial.

166. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) provide adequate and lifetime credit monitoring to Plaintiff and all Class Members.

COUNT II

UNJUST ENRICHMENT

(On Behalf of Plaintiff and the Class)

167. Plaintiff re-alleges and incorporates by reference all the allegations contained in paragraphs 1 through 141 above, as if fully set forth herein.

168. Plaintiff pleads this claim for unjust enrichment in the alternative to the breach of implied contract count above.

169. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided their PII to Defendant and Defendant used and depended on that PII to operate its business, which specifically includes data management and protection services. In exchange, Plaintiff and Class Members should have had their PII protected with adequate data security.

170. Defendant knew Plaintiff and Class Members conferred a benefit upon it, and accepted that benefit by retaining the PII and using it to generate revenue.

171. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided Defendant.

172. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, unjustly profited from the value that collecting, storing, using, and transmitting their PII provided Defendant.

173. Defendant acquired the PII through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

174. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own pocket. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant' decision to prioritize its own financial condition over the requisite security and the safety of customers' PII.

175. Under the circumstances, it would be unjust for Defendant to retain the benefits that Plaintiff and Class Members conferred upon it.

176. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injuries and damages as set forth herein.

177. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful

conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

COUNT III

BREACH OF THIRD-PARTY BENEFICIARY CONTRACT

(On Behalf of Plaintiff and the Class)

178. Plaintiff re-alleges and incorporates by reference paragraphs 1 through 141 above as if fully set forth herein.

179. Upon information and belief, Defendant entered into uniform written contracts with its clients to provide enterprise resource planning and data management services that entailed Defendant's collection, use, and storage of Plaintiff's and Class Members' PII.

180. Pursuant these contracts, Defendant received from its clients and maintained Plaintiff's and Class Members' PII in the course of providing enterprise resource planning and data management services, which it could not perform without receiving and maintaining such PII.

181. Pursuant to these contracts, Defendant's clients agreed to provide Defendant with compensation and Plaintiff's and Class Members' PII.

182. In exchange, Defendant agreed, in part, to implement adequate data security measures to safeguard Plaintiff's and Class Members' PII from unauthorized disclosure.

183. Upon information and belief, Defendant's contracts with its clients each contained a provision requiring Defendant to implement and maintain reasonable security procedures and practices appropriate to the nature of PII it collected, and to protect the PII from unauthorized access, use, or disclosure.

184. These contractual obligations for reasonable data security and nondisclosure that Defendant assumed vis-à-vis its clients were made expressly for

the benefit of Plaintiff and Class Members, as Plaintiff and Class Members were the intended third-party beneficiaries of these contracts.

185. Defendant knew if it breached its contractual obligations to adequately safeguard its clients' customers' and/or employees' PII, the individuals to whom that data pertained—Plaintiff and Class Members—would be harmed.

186. Defendant breached these contracts by, among other acts and omissions, (a) failing to use reasonable data security measures and (b) failing to implement adequate protocols sufficient to protect Plaintiff's and Class Members' PII from unauthorized disclosure.

187. As a direct and proximate result of Defendant's breaches of these contracts, Plaintiffs and Class Members have suffered and will continue to suffer injuries as set forth herein, and are entitled to damages sufficient to compensate for the losses they sustained as a direct result thereof.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Randall Wright, individually and on behalf of all others similarly situated, prays for judgment as follows:

A. An Order certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, exemplary, and punitive damages, as allowed by law;

C. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

D. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

E. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

F. Awarding attorneys' fees and costs, as allowed by law,

G. Awarding pre- and post-judgment interest, as provided by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and,

I. Any and all such relief to which Plaintiff and the Class are entitled.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues to triable.

Dated: March 17, 2025

Respectfully submitted,

By: */s/ Kristen Lake Cardoso*

Kristen Lake Cardoso
KOPELOWITZ OSTROW P.A.
Kristen Lake Cardoso (CA Bar No. 338762)
cardoso@kolawyers.com
Jeff Ostrow (*pro hac vice* forthcoming)
ostrow@kolawyers.com
One West Las Olas, Suite 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100

Attorneys for Plaintiff and the Putative Class